REMARKS/ARGUMENTS

Favorable consideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 8-11 and 13-14 are pending with Claims 1-7 and 12 withdrawn from consideration.

In the Official Action Claims 8, 9, 13 and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Shamir (EP 0325238) in view of Schneier (Applied Cryptography Protocols, Algorithms and Source Code in C, 2nd Edition, pages 249 and 250); and Claims 10 and 11 were indicated as containing allowable subject matter.

Applicants acknowledge with appreciation the indication of allowable subject matter.

Briefly recapitulating, amended Claim 8 is directed to an authentication process involving a first device, which possesses a public key v and a secret key s, and a second device, which knows the public key v, the first and second entities being provided with means to exchange zero-knowledge information and to carry out cryptographic calculations on the zero-knowledge information. The public and secret keys are related by an operation modulo n, where n is an integer. The modulus n is specific to the first device. Calculations are carried out modulo n wherein in the process the modulo n operation is of $v=s^{-t}$ (mod n), t is a parameter and the modulo n calculations are performed according to the "Chinese remainders" method. The modulus n is the product of two primes of similar size.

Shamir describes a residue modulo n calculation. However, as noted in the Official Action, Shamir is silent about the use of the Chinese remainder. Schneier discloses a variety of cryptography protocols and discloses the use of the Chinese Remainder theorem. However, Schneier fails to disclose or suggest using the Chinese Remainder theorem in an authentication process. Applicants submit that a person having an ordinary skill in the art would not find in Schneier any indication or suggestion to perform the residue modulo n calculation in Shamir's invention by means of calculation according to the Chinese remainder method.

Furthermore, while Shamir describes a modulus n which is the product of primes (instead of being itself a prime), both Shamir and Schneier fail to disclose or suggest a calculation where n is the product of two primes, p and q and that p and q are of the same order. That is, both Shamir and Schneier fail to disclose or suggest a calculation where modulus n is the product of two primes of similar size, as recited in amended Claim 8. When p and q are of similar size, each of the calculations (y_p and y_q) is about 8 times faster than the calculation of $y =x^e$ (mod n) when n and e are of similar size, 4 times faster when the size of e is lower or equal to the size of p.

On the whole, the use of the Chinese remainder leads to an acceleration of calculation by factor ranging from 3 to 4 or 1, 5 to 2 depending on the size of e with regard to n and to p. Furthermore, when the number of primes factors (assumes to be' of similar sizes) is larger than 2 and equal to k, the acceleration factor is nearing k^2 in the first case (e and n of similar size) and close to k in the seconds case (e is lower than or equal to p)

Regarding the Examiner's comments on Applicants' previously filed remarks, Applicants continue to traverse the rejection of the pending claims in view of Shamir. Applicants note that the rejection is based upon an example disclosed in Shamir in which n is taken equal to the product of two prime numbers p and g, where p=3 mod 8 and g=7 mod 8, so that public keys vj are automatically quadratic residues mod n. Applicants submit this mathematical characteristic is different from the one claimed in the present invention in which prime numbers p and g are of **similar size**. Using Shamir's criterion, one can consider for example p=3 and g=8*100,000+7=80007, such that g is 200,000 times greater than p. Consequently, in the example of Shamir p and g do not necessarily have a **similar size** as is required by Applicants' claimed invention.

MPEP §706.02(j) notes that to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. Also, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Regarding cancelled Claim 12 (and now amended Claim 8), Applicants submit that the Official Action does not present a *prima facie* case of obviousness because both there is no motive to combine Shamir and Schneier achieve the features of Applicants' claimed invention.

Accordingly, in view of the present amendment and in light of the previous discussion, Applicants respectfully submit that the present application is in condition for allowance and respectfully request an early and favorable action to that effect.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599

Michael E. Monaco
Registration No. 52,041

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)